

IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF VIRGINIA
LYNCHBURG DIVISION

IN THE MATTER OF THE SEARCH OF THE
2011 NISSAN SENTRA BEARING VEHICLE
IDENTIFICATION NUMBER
3N1AB6AP9BL713761

Case No. 6:23mj13

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason P. McCoy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the vehicle seized from Derrick Loi on February 24, 2023, and described in **Attachment A** of this affidavit (the “SUBJECT VEHICLE”), specifically the contents of the vehicle, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2422, 2251, 2252, and 2252A, more specifically described in **Attachment B** of this affidavit.

2. Your affiant is a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code. I have been employed with the FBI since July 2019 and as a law enforcement officer since 2007. Prior to joining the FBI, I was a Special Agent with the United States Air Force Office of Special Investigations and began conducting federal criminal investigations after completing the Federal Law Enforcement Training Center’s Criminal Investigator Training Program in September 2013. I have extensive experience investigating a myriad of crimes, including criminal and national

security investigations. As an FBI SA I have received extensive training in the investigation of violations of federal and state law. I am currently assigned to the FBI Richmond Division, Lynchburg Resident Agency, where as part of my duties, I investigate criminal violations relating to child exploitation, to include enticement, in violation of 18 U.S.C. § 2251 and 18 U.S.C. § 2422, as well as child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A. I have experience in the area of child pornography and child sexual exploitation investigations and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media. I also have experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search of vehicles and seizure of evidence found within.

3. As an FBI agent, I am authorized to conduct investigations, carry firearms, execute warrants, make arrests, and perform other duties sanctioned by the FBI. Over the course of my career, I have conducted interviews and secured other relevant information, using a variety of investigative techniques. I am a federal law enforcement officer under the applicable provisions of the U.S.C. and under Rule 41(a) of the Federal Rules of Criminal Procedure. As a result, I am authorized to apply for this search warrant.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. As set forth below, there is probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422; (enticement of an individual who as not attained the age of 18); 2251(A) (production of child pornography), 2252(a)(2) and (b)(1) (receipt or distribution of a visual depiction of a minor engaged in sexually explicit conduct); 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct); and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of and access with intent to view child pornography) are presently located inside the SUBJECT VEHICLE.

DEFINITIONS

6. The following definitions apply to this affidavit:

a. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

c. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. “Discord” is a free communications app that allows its users to share voice, video, and text chat with persons on the Internet as well as browse and share any website content with those whom the user selects while still within the Discord platform. Unlike other messaging apps, Discord usernames - not phone numbers - are the basis for Discord user accounts. Discord usernames are unique, can never be replicated, and are the only publicly available identifier Discord can use to identify a Discord account to law enforcement. The company cannot identify users using phone numbers, first and last name (display name), or email address.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO ACCESS WITH INTENT
TO VIEW CHILD PORNOGRAPHY**

7. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who access online child sexual abuse and exploitation material via the Internet:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain child pornographic material in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain those materials and child erotica for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information (e.g., online messaging accounts, email addresses, etc.) of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. Even if the target uses a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than not that evidence of this access will also be found on digital devices other than the portable device (for reasons including the frequency of "backing up" or "syncing" mobile phones to computers or other digital devices).

CASE BACKGROUND AND PROBABLE CAUSE

8. On February 24, 2023, at approximately 10:25 PM, I received a call from the Lynchburg Police Department notifying me that the Lynchburg Communications Center received a report that 28-year-old Derrick Loi had traveled from the state of New York for the purpose of

engaging in sexual intercourse with a 14-year-old female (the “victim”). The complainant stated that Loi was waiting to meet the victim on McVeigh Road in Lynchburg, Virginia, which is within the Western District of Virginia. Loi told the victim he would take her to a Quality Inn to have sex. Officers from the Lynchburg Police Department responded to the victim’s address to make contact with her while additional officers responded to McVeigh Rd, where Loi was parked. Loi was initially identified by a photograph provided to Officers by the victim and later was fully identified as 26-year-old Derrick Loi of Lakeville, NY. Officers placed him into investigative detention.

9. Officers learned from the victim that she and Loi had been in communication for approximately two and a half weeks via Discord. Officers were provided consent to search the victim’s laptop by her father. On the laptop, the officers reviewed the Discord profile associated with username NicoleIO#XXXX but did not observe any communications between the victim and Loi. The victim stated she had deleted the conversations prior to the officers’ arrival. The victim did not recall Loi’s username but did remember it started with the word “call.” The victim told the officers that her conversations with Loi were sexual in nature and that Loi asked her to send pornographic photos of herself, which she did. Loi told the victim he wanted to “rape her” and instructed the victim to leave a note saying she was staying at a friend's house. The victim stated to the officers that she told Loi she was 14 years old.

10. After confirming Loi made a hotel reservation in the Lynchburg area, the Lynchburg police transported Loi to the Lynchburg Police Department, where an interview of Loi was conducted. During the interview, Loi confirmed he had driven from New York to Lynchburg, Virginia, to meet someone he had been speaking to online. Loi did not recall the username NicoleIO#XXXX and said he believed he was talking to someone named “Katie.” Loi told the interviewing officer that his Discord usernames were “LPKensei” and “Callthevoid.” Loi stated

he and “Katie” discussed “hooking up,” but he denied knowing how old she was. Loi stated he had requested and received photographs of a “lewd nature” from “Katie.” Loi stated he and “Katie” used the Discord chat, video, and audio features.

11. Once the interview was concluded, the interviewing officer placed Loi under arrest. A Samsung cell phone with IMEI 350319816759476, which was located on Loi’s person, was seized by the Lynchburg Police Department.

12. During a search of Loi’s vehicle, officers discovered an HP Specter Laptop with Serial Number 5CD0188SN7, two USB thumb drives, a bag containing various sex toys and lubricant, a bag containing a box of condoms, and a Plan B pill used for emergency contraception. Upon opening the trunk area, officers observed a vinyl or rubber shower liner covering most of the carpeted floor space in the trunk. There was a flattened cardboard box on top of the liner that had a red stain from an unknown substance. Officers also observed large plastic storage bags along the right side of the trunk.

13. On February 28, 2023, I reviewed reports provided by the Lynchburg Police Department and opened an investigation into this matter. The victim’s laptop was transferred to FBI custody, and I sought and obtained written consent from the victim’s father to search the contents of the laptop computer that the victim had used to communicate with Loi.

14. While reviewing the contents of the victim’s laptop on March 15, 2023, agents discovered a Discord profile logged into the Discord web browser on the device, which enabled agents to review the associated user’s chat history. The username on the account was “kaiteee#XXXX.” While reviewing the contents of this account, agents discovered communications with user “Callduvide#XXXX” (Callthevoid; “du vide” is French for the void). These communications made clear that “kaiteee#XXXX” was a Discord profile being used by the

victim and that “Callduvide#XXXX” was a Discord profile being used by Loi. Agents observed that on February 14, 2023, the victim, using the “kaiteee#XXXX” username, stated that she was 14 years old. Throughout the conversation, “Callduvide#XXXX” repeatedly requested pornographic images from the victim and discussed traveling from New York to Lynchburg, Virginia, to engage in sexual intercourse with the victim. On February 14, 2023, “Callduvide#XXXX” stated “Ooh I can’t wait to try out your kiddie holes...”. “Callduvide#XXXX” provided money to the victim in exchange for child pornography and, in one instance, the victim sent images described as herself at the age of 12 years old. “Callduvide#XXXX” suggested he could be her “sugar daddy” and pay her weekly. On February 24, 2023, “Callduvide#XXXX” told the victim “take a pic of ur pussy rn.” The victim responded by sending an image depicting herself nude, exposing her genitals.

15. During the conversation, “Callduvide#XXXX” discussed taking the victim’s virginity and discussed the victim taking birth control. He told the victim he was bringing vodka and sex toys. On February 23, 2023, he sent a photograph of sex toys, lubricant, and a “Plan B” box, and on February 24, 2023, he sent a photograph of a vodka bottle. “Callduvide#XXXX” discussed with the victim the possibility of staying in a hotel overnight and questioned the victim about her parents’ response if she did not return home. “Callduvide#XXXX” instructed the victim to tell her parents she was staying with a friend the night she planned to meet him. “Callduvide#XXXX” asked the victim if they could film their sexual encounter when he traveled down to have sex with her and continued by stating “...hopefully I get good footage.” On February 24, 2023, he told the victim “I’m so excited to fuck you” and then told the victim when he initially arrived at McVeigh Road. He then left to check into the hotel before returning to McVeigh Road. The final message from “Callduvide#XXXX” was received at approximately 9:41 PM.

16. “Callduvide#XXXX” told the victim that some of the images that she sent were “nothing I haven’t seen before.” He sometimes referred to the victim as a “seller” and mentioned interacting with other “sellers” on the internet.

17. On March 23, 2023, I spoke with Lynchburg Police Department Investigator T. Hall who initially conducted a search of the TARGET VEHICLE. Hall stated that still within the vehicle are notebooks, a duffle bag, a bottle of pink alcohol with a black label, a roll of saran wrap, and the plastic and stained cardboard noted inside the trunk of the vehicle. Of note, the description of the bottle of alcohol described by Hall matched the photograph observed by agents reviewing the Discord chat between Loi and the victim.

18. The facts as outlined above provide me with a reasonable belief that the SUBJECT VEHICLE contains evidence that Loi, the user of Discord username “Callduvide#XXXX,” produced, possessed, received, and distributed child pornography, by means of the internet, with a minor residing in the Western District of Virginia. There is also a reasonable belief that evidence of Loi’s travel from New York to the Western District of Virginia, to engage in sexual intercourse with the victim (a minor), exists in the SUBJECT VEHICLE. Lastly, there is a reasonable belief that evidence exists in the SUBJECT VEHICLE related to other victims of similar crimes, which could be further identified.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

19. I anticipate executing this warrant on the SUBJECT VEHICLE to search for physical evidence of the violations previously noted. Specifically, I aim to seize the bottle of vodka as it shows further proof that Loi was the owner and controller of the Discord username “Callduvide#XXXX” at the time of his arrest. I also aim to seize the section of cardboard containing the unknown red stain for future analysis and identification. I intend to use non-

intrusive techniques to collect samples from inside the trunk and passenger compartment, such as DNA, hair, and fiber samples, which can be used to identify potential victims of similar crimes. The entire contents of the TARGET VEHICLE, to include any containers remaining therein, will be searched for further evidence of the violations under investigation, to include any further digital devices that may be hidden within the vehicle.

20. If any other digital devices are found within the vehicle, I submit that there is probable cause to believe child pornography materials will be stored on the computers or storage mediums, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this

forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

21. As further described in Attachment B, this application seeks permission to locate not only physical evidence, but evidence of vehicle ownership and registration, which further shows the vehicle’s use and travel in interstate commerce. Additionally, if further electronic devices are discovered, this application seeks permission to locate computer files that might serve as direct evidence of the crimes described in the warrant, as well as forensic electronic evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any electronic devices discovered during this search because: data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices, or other external storage media, and the times the computer was in use. Computer file systems can record information about

the dates files were created and the sequence in which they were created, although this information can later be falsified.

22. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner.

23. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated

into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement). A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

24. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

25. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present

on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

CONCLUSION

Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located in the SUBJECT VEHICLE, which is described in Attachment A. I respectfully request that this Court issue a search warrant for the property described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

JASON
MCCOY
Digitally signed
by JASON MCCOY
Date: 2023.03.27
08:49:44 -04'00'

Jason P. McCoy
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me this 29th day of March, 2023.

Robert S. Ballou

The Honorable Robert Ballou
UNITED STATES DISTRICT JUDGE